

REMARKS

Reconsideration of the issues raised in the Office Action dated August 11, 2009 is respectfully requested in light of the amendments to the specification and the claims, and the remarks presented herewith. The issues are addressed below in the order in which they are presented in the Office Action.

Status of the Claims

Claims 1-53 are pending in the present application. No claims have been amended, canceled, or added by this Response, but the claims have been reproduced in the attached Listing of Claims for convenience.

Objection to Specification

The disclosure has been objected to because the use of the trademarks BLUETOOTH® and SMARTMEDIA® in the application has been identified as requiring correction with respect to proper capitalization and accompaniment by generic terminology.

In the amendments to the Specification presented herewith, the Specification has been amended to ensure proper capitalization and accompaniment by generic terminology.

It is respectfully submitted that amendments to the Specification adequately address the identified objections to the Specification, and it is respectfully requested that the stated objections be withdrawn.

Claim Rejections – 35 U.S.C. 102

Claims 1 – 3, 5, 14 – 17, 19 – 23, 25, 34 – 38, and 41 – 43 have been rejected under 35 U.S.C. 102(b) as being anticipated by Ohashi et al. (U.S. Patent No. 5,761,309) (“Ohashi”). This rejection is respectfully traversed.

In support of the traversal of this rejection, a Declaration of Charles William Debney under 37 C.F.R. 1.132 (“the Declaration”) is submitted herewith. Mr. Debney, in addition to being one of the inventors listed in the present application, is well qualified by both education

and experience to present technical evidence with respect to the subject matter of the claims of the present application. See: paragraphs 2-7 of the Declaration.

As explained by Mr. Debney in paragraphs 8-10 of the Declaration, the present invention relates to the facilitation and authentication of transactions. In embodiments of the invention, transactions between a data processing apparatus (such as a personal computer), or a user thereof, and a (possibly remote) third party are facilitated and authenticated, and such facilitation and authentication may also involve the facilitation and authentication of a payment or data transfer to be made by or on behalf of the user to the third party. See: paragraph [0001] of the present application, published as U.S. Patent Application Publication No. US 2006/0112275 A1.

Independent claim 1 recites “a device for connection to a data processing apparatus, the device including, authentication storage means operatively coupled thereto for storing predetermined authentication information respective to a user, ... the device, when operatively coupled to the authentication storage means, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means, ...” (emphasis added).

Independent claim 21 recites “a method for authenticating a transaction with a data processing apparatus in which the data processing apparatus has operatively associated with it a security device which in turn has operatively associated with it authentication storage means for storing predetermined authentication information respective to a user, ... the device, when operatively coupled to the authentication storage means, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means, ...” (emphasis added).

Independent claim 42 recites “a device including authentication storage means for controlling access to predetermined authentication information stored on the authentication storage means, the device including means for coupling the device to a data processing apparatus to allow the authentication information to be used to authenticate a transaction performed by the data processing apparatus, ... the device, when operatively coupled to the authentication storage means, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate the transaction by the user with the data processing apparatus,” (emphasis added).

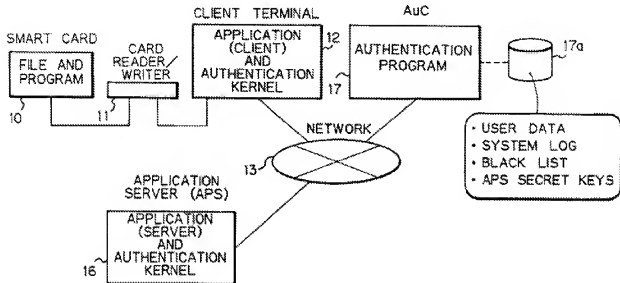
In the Office Action, the Examiner’s position was stated as follows: “Regarding claims 1, 21, and 42, Ohashi disclosed a device (card reader 11) for connection to a data processing apparatus (client terminal 12), the device (card reader 11) including authentication storage means (smart card 10) operatively coupled thereto for storing predetermined authentication information respective to a user (Ohashi Col. 12 Lines 1-29), ... the device (card reader 11), when operatively coupled to the authentication storage means (smart card 10), being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means (AuC data) to carry out an authentication process via a communication link (network 13) with the authenticating means (AuC data) in the said telecommunications system (authentication center) whereby to authenticate a subsequent transaction by the user with the data processing apparatus (client terminal 12) (Ohashi Col. 12 Lines 1-29), and which involves use of the data carded by the authentication storage means (smart card 10) (Ohashi Col. 12 Lines 1 -29),” (Office Action, page 4). This allegation is respectfully traversed.

Ohashi relates to an authentication system for identifying a user by a network when the user intends to get network services (col. 1, lines 4-6).

As explained by Mr. Debney in Paragraph 12 of the Declaration, FIG. 6 of Ohashi (reproduced below) is a block diagram schematically showing an embodiment of an authentication system of a purported invention (col. 11, lines 7-9). In the figure, reference numeral 10 denotes a smart card provided with a program and a file and possessed by each user,

11 denotes a card reader/writer for reading information from or writing information to the smart card 10, and 12 denotes a client terminal connected to the reader/writer 11, provided with client side application and authentication kernel, respectively (col. 11, lines 10-16).

Fig. 6



For convenience, the passage of Ohashi at column 12, lines 1-29 is reproduced below:

For the card user, a PIN code has been previously defined, and this defined PIN code has been stored in the smart card 10. The user inputs his PIN code through the client terminal 12 into the smart card 10 so that coincidence between the input PIN code and one stored in the smart card 10 is checked. This check of the PIN code is executed by internal operation of the smart card 10. If PIN code input is successively failed three times, the smart card 10 permits no more access and thus the authentication procedure terminates. Since the memory in the smart card 10 is a nonvolatile storage, the number of the past successive PIN input failure will be held even if the power is off. This storage will be cleared if PIN code check is succeeded within successive three times inputs.

After the smart card 10 is activated by local verification between the user and the smart card 10, authentication processes are carried out with following two phase sequence.

A first phase is request and issuance of a user certificate. In this first phase, the user side (smart card 10) requests the AuC 17 to

issue a certification information (user certificate) which verifies him. The issued user certificate which has a valid period is stored in the smart card 10. Prior to accessing the AuC 17, the user side (smart card 10 or client terminal 12) confirms the validity of the already obtained user certificate. As long as the user certificate is valid, the authentication processes can be jumped to a next second phase without accessing the AuC 17. This causes throughput in the AuC 17 to decrease.

As explained by Mr. Debney in paragraph 14 of the Declaration, the passage of Ohashi at column 12, lines 1-29 describes the conventional mechanism by which a client terminal (e.g., a telecommunication handset) checks that a user has input a PIN that matches the PIN stored on a smartcard/SIM. The scenario set out in Ohashi is thus entirely different than the subject matter of the present invention and would not fall within the scope of a “transaction” as recited in the claims of the application.

Further, the “authentication center (AuC) 17” of Ohashi cannot reasonably be equated to a “telecommunications system” because Ohashi only describes the authentication center (AuC) 17 as having an authentication program for verifying the user (col. 11, lines 34-39), which cannot be construed as a disclosure that the authentication center (AuC) 17 is or performs the functions of a telecommunications system, as recited in the claims of the application. As described in response to the previous Office Action, the authentication information stored by the authentication storage means corresponds to information which is used to authenticate the user's telecommunications handset with the telecommunication system. However, the authentication process for authenticating the transaction by the user with the data processing apparatus does not require use of the user's telecommunication handset nor does it require the telecommunications handset to be actually authenticated by the information in relation to the telecommunications system.

The claimed invention makes use of the predetermined authentication information on the authentication storage means and uses this for authenticating a transaction with data processing apparatus where no telecommunications handset is involved. In the embodiment described in the Specification, the user's SIM (authentication storage means) performs authentication using the predetermined authentication information without involvement of the user's telecommunications terminal. There is no suggestion of such an arrangement in Ohashi.

Ohashi discloses that the “other client terminals” (col. 11, lines 30-33), which are read in the Office Action as the “telecommunications terminal” of the claims, are “a plurality of client terminals having similar construction as the terminal 12 and connected via respective communication lines” (emphasis added). Ohashi does not disclose any telecommunications functionality of such “other client terminals” or any distinction between such “other client terminals” (read as the telecommunications terminal recited in the claims) and the “client terminal 12” (read as the data processing apparatus recited in the claims). Accordingly, it is respectfully submitted that such “other client terminals” cannot be reasonably interpreted as the “telecommunications terminal” recited in the claims of the present application.

The present application pre-dates any published proposal of which the Applicant is aware where the SIM/authentication storage means is used separately from the telecommunications terminal. That is, the predetermined authentication information on the SIM, corresponding to information that is used to authenticate a telecommunications terminal with a common telecommunications system, is used to authenticate a transaction with a data processing apparatus by operatively associating the authentication storage means/SIM with the data processing apparatus, without the user's telecommunications terminal.

At the priority date of the present application, there was a prejudice in the mobile telecommunications art against using an authentication storage means/SIM separately from a telecommunications terminal. Such a use of a SIM was never envisaged prior to the present application. The present invention provides a significant technical advantage of providing secure authentication, for example using the challenge and response SIM authentication between the SIM and the authenticating means of the common telecommunications system, to authenticate a transaction using a data processing apparatus with which the authentication storage means/SIM is operatively coupled. The authentication requires processing of the challenge and response to be performed at both ends of the communication channel over which the transaction is authenticated. The present invention enables secure and reliable authentication of transactions to be performed without developing new authentication infrastructure.

Dependent claims 2 – 3, 5, 14 – 17, 19 – 20, 22 – 23, 25, 34 – 38, 41, and 43 each depend from one of independent claims 1, 21 and 42 and are also allowable for at least the reasons discussed above.

Claim Rejections – 35 U.S.C. 103

Claims 18, 39 – 40, 46 – 51, and 53 have been rejected as being unpatentable over Ohashi. Claims 4, 6 – 13, 24, 26 – 33, 44 – 45, and 52 have been rejected as being unpatentable over Ohashi in view of Caputo et al. (U.S. Patent No. 5,778,071) (“Caputo”). These rejections are respectfully traversed.

Claims 4, 6 – 13, 18, and 46 – 48 depend from amended independent claim 1, claims 24, 26 – 33, 39 – 40, and 49 – 52 depend from amended independent claim 21, and claims 44 – 45 and 53 depend from amended independent claim 42.

It is respectfully submitted that claims 18, 39 – 40, 46 – 51, and 53 are allowable over Ohashi, alone, for at least the reasons provided above in support of the allowability of independent claims 1, 21 and 42 over Ohashi.

Further, with respect to claims 4, 6 – 13, 24, 26 – 33, 44 – 45, and 52, it is respectfully submitted that Caputo clearly does not compensate for the above-described deficiencies of Ohashi as a reference against the independent claims. Thus, it is respectfully submitted that claims 4, 6 – 13, 24, 26 – 33, 44 – 45, and 52 are allowable over Ohashi in view of Caputo for at least the reasons provided in support of the allowability of independent claims 1, 21 and 42.

Given the significant technical advantages of the present invention, and the absence of any prior art disclosing or suggesting the claimed authentication arrangement, it is respectfully submitted that there is simply no reason that a person of ordinary skill in the art at the time of the invention would modify any prior art document or “telecommunication authentication standards” in order to arrive at the present invention.

Application No. 10/531,430
Amendment dated September 10, 2010
Notice of Appeal dated February 11, 2010
Office Action dated August 11, 2009

Allowance of the application in its present form is thus respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Date: September 10, 2010

Signed By
Attorney of Record

/jeffrey a. haeberlin, reg. no. 40,630/

Name: Jeffrey A. Haerberlin
Registration No.: 40,630

STITES & HARBISON PLLC ♦ 1199 North Fairfax St. ♦ Suite 900 ♦ Alexandria, VA 22314
TEL: 703-739-4900 ♦ FAX: 703-739-9577 ♦ CUSTOMER NO. 881